IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

KAZANDRA BARLETTI, individually, as a natural parent and next friend of A.B.T., a minor, and on behalf of all others similarly situated., Plaintiff, v. CONNEXIN SOFTWARE, INC. d/b/a OFFICE PRACTICUM, Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Kazandra Barletti, as a natural parent and guardian of A.B.T. (together, "Plaintiff"), individually and on behalf of all others similarly situated (collectively, "Class Members"), by and through her attorneys, brings this Class Action Complaint against Defendant Connexin Software, Inc. d/b/a Office Practicum ("CSI" or "Defendant") and alleges upon personal knowledge as to herself and A.B.T. and upon information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against CSI for its failure to secure and safeguard A.B.T.'s and approximately 2.2 million other individuals' personally identifiable information ("PII") and personal health information ("PHI") (collectively, "Private Information").

2. Defendant is a business vendor that provides pediatric physician practice groups with electronic medical records, practice management software, billing services, and business analytic tools.

3. As a condition of receiving services, CSI's medical provider customers and their patients are required to provide and entrust CSI with sensitive information, including their Private

Information. The Private Information that CSI collects and maintains includes names of children and parents, dates of birth, Social Security numbers, medical information (including diagnoses), provider's names, medical record numbers, health insurance information, and treatment information.

4. On or around August 26, 2022, CSI detected encrypted files on some of its systems and began investigating the incident. By September 13, CSI determined that an unauthorized party had accessed certain CSI servers. (the "Data Breach").

5. On November 14 and 17, 2022, CSI provided a summary of its investigation to the Attorneys General of Montana and Texas, respectively, reporting that the incident affected thousands of individuals in those states alone.[1] CSI also made available a "substitute notice" for individuals who have insufficient or out-of-date contact information.[2] Upon information and belief, CSI notified approximately 2.2 million patients nationwide that their Private Information had been compromised in the Data Breach.[3]

6. CSI's notice letter provided scant detail, particularly considering the size and scope of the Data Breach and the sensitivity of Plaintiff's and Class Members' compromised information. CSI's notice states, in relevant part, that CSI "detected a data anomaly on our internal network. . . immediately launched an investigation and engaged third-party forensic experts to determine the nature and scope of the incident" and that "an unauthorized party was able to access

[1] *See* https://oagtx.force.com/datasecuritybreachreport/apex/DataSecurityReportsPage (267,296 Texas residents affected; last visited December 14, 2022); https://dojmt.gov/consumer/databreach/ (17,199 Montana residents affected; last visited December 14, 2022).
[2] "Unauthorized Access to Internal Computer Network at Connexin Software, Inc." https://www.officepracticum.com/substitute-notice/ (last accessed December 13, 2022).
[3] https://healthitsecurity.com/news/third-party-data-breach-impacts-119-pediatric-practices-2.2m-patients (last visited December 14, 2022).

an offline set of patient data used for data conversion and troubleshooting. Some of that data was removed by the unauthorized party."

7. CSI's notice did not disclose how long cybercriminals had access to its systems, how it discovered the encrypted files on its computer systems, the means and mechanism of the cyberattack, the reason for the delay in notifying Plaintiff and the Class of the Data Breach, how CSI determined that the Private Information had been "removed" by the unauthorized actor, and, importantly, what steps CSI took following the Data Breach to secure its systems and prevent future cyberattacks.

8. CSI reported that the scope of compromised information involved included: "(1) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth); (2) Social Security Numbers ("SSNs"), (3) health insurance information (payer name, payer contract dates, policy information including type and deductible amount and subscriber number); (4) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); and (5) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider)."[4]

9. The Data Breach was the direct result of CSI's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect patients' Private Information from the foreseeable threat of a cyberattack.

10. By taking possession and control of Plaintiff's and Class Members' Private Information for its own pecuniary benefit, CSI assumed a duty to Plaintiff and Class Members to

[4] https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-712.pdf (last visited December 14, 2022).

implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiff's and Class Members' Private Information against unauthorized access and disclosure. CSI also had a duty to adequately safeguard this Private Information under industry standards and duties imposed by statutes, including HIPAA regulations and Section 5 of the Federal Trade Commission Act ("FTC Act"). CSI breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect patients' Private Information from unauthorized access and disclosure.

11. As a result of CSI's inadequate security and breach of its duties and obligations, the Data Breach occurred, Plaintiff and over two million Class Members suffered injury and ascertainable losses in the form of out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, the diminution in value of their personal information from its exposure, and the present and imminent thread of fraud and identity theft, among other things. This action seeks to remedy these failings and their consequences to Plaintiff and Class Members.

12. The injury to Plaintiff and Class Members was compounded by the fact that CSI did not notify patients that their Private Information was subject to unauthorized access and exfiltration until almost three months after the initial "data anomaly" was detected, and Defendant still has not revealed the full scope of the Data Breach. CSI's failure to timely notify the victims of its Data Breach meant that Plaintiff and Class Members were unable to take affirmative measures to prevent or mitigate the resulting harm. In some cases, it did not notify patients at all.

13. Despite having been accessed and exfiltrated by unauthorized criminal actors, Plaintiff's and Class Members' sensitive and confidential Private Information still remains in the

possession of CSI. Absent additional safeguards and independent review and oversight, the information remains vulnerable to further cyberattacks and theft.

14. CSI disregarded the rights of Plaintiff and Class Members by, *inter alia*, failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiff and Class Members prompt and adequate notice of the Data Breach.

15. In addition, CSI and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had CSI properly monitored these electronic systems, it would have discovered the intrusion sooner or prevented it altogether. Moreover, it appears that the Private Information was stored unencrypted as, had proper encryption practices been implemented, the cyber attacker would have exfiltrated only unintelligible data.

16. The security of Plaintiff's and Class Members' identities is now at risk because of CSI's wrongful conduct as the Private Information that CSI collected and maintained is now in the hands of data thieves. This present risk will continue for the course of their lives.

17. Armed with the Private Information accessed in the Data Breach, data thieves can commit a wide range of crimes including, for example, opening new financial accounts in Class Members' names, taking out loans in their names, using Class Members' identities to obtain government benefits, filing fraudulent tax returns using their information, obtaining driver's

licenses in Class Members' names, obtaining medical services, insurance coverage and medications, and giving false information to police during an arrest.

18. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a present, imminent, and continuing risk of fraud and identity theft. Among other measures, Plaintiff and Class Members must now and in the future closely monitor their financial accounts and medical records to guard against identity theft. Further, Plaintiff and Class Members will incur out-of-pocket costs to purchase credit monitoring and identity theft protection and insurance services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

19. Plaintiff and Class Members will also be forced to expend additional time to review credit reports and monitor their financial accounts and medical records for fraud or identity theft. Due to the fact that the exposed information potentially includes Social Security numbers ("SSNs") and other immutable personal details, Plaintiff and Class Members are at risk of identity theft and fraud that will persist throughout the rest of their lives.

20. Plaintiff brings this action on behalf of herself and individuals in the United States whose Private Information was exposed as a result of the Data Breach. Plaintiff and Class Members seek to hold CSI responsible for the harms resulting from the massive and preventable disclosure of such sensitive and personal information. Plaintiff seeks to remedy the harms resulting from the Data Breach on behalf of herself and all similarly situated individuals whose Private Information was accessed and exfiltrated during the Data Breach.

21. Plaintiff and Class Members thus seek actual damages, statutory damages, restitution, injunctive and declaratory relief (including significant improvements to CSI's data

security protocols and employee training practices), reasonable attorneys' fees, costs, expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

PARTIES

22. Plaintiff Kazandra Barletti is a resident and citizen of the Commonwealth of Pennsylvania and resides in Croydon, PA. Ms. Barletti's child, A.B.T., has been a patient at We Care Pediatrics, PC, and has visited frequently in recent months. We Care Pediatrics, PC is identified on CSI's website as one of the practices whose patients were victimized by the Data Breach. Ms. Barletti received a letter dated December 6, 2022 notifying her that her daughter A.B.T.'s personal information may have been compromised in the data breach.

23. Defendant Connexin Software, Inc. is a Delaware corporation with its principal place of business located at 602 W. Office Center Drive, Suite 350, Fort Washington, Pennsylvania, 19034.

24. CSI refers to itself as "[t]je industry leader in pediatric-specific Health Information Technology Solutions" and claims that it "provides pediatric-specific health information technology solutions for independent pediatric practices."[5] Due to the nature of these services, CSI acquires and electronically stores patient Private Information.

JURISDICTION AND VENUE

25. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class is a citizen of a different state than Defendant, there are more than 100 Members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

[5] Office Practicum LinkedIn page. https://www.linkedin.com/company/officepracticum/about/ (last accessed December 13, 2022).

26. This Court has personal jurisdiction over CSI because CSI maintains its principal place of business in Pennsylvania and conducts substantial business in Pennsylvania and in this district through its principal place of business; engaged in the conduct at issue herein from and within this District; and otherwise has substantial contacts with this District and purposely availed itself of the Courts in this District.

27. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) and (2) because CSI resides in this district, and this district is where a substantial part of the acts, omissions, and events giving rise to Plaintiffs' claims occurred.

FACTUAL ALLEGATIONS

A. Overview of CSI

28. CSI is a software and business services company incorporated in Maryland with its principal place of business in Fort Washington, Pennsylvania. CSI provides electronic medical records, practice management software, billing services, and business analytic tools to pediatric physician practice groups. The company provides a range of services to its clients, including financial solutions, patient engagement, and clinic operations.

29. In the regular course of its business, CSI collects and maintains the Private Information of patients, former patients, and other persons through its healthcare provider customers to whom it is currently providing or previously provided health-related or other services.

30. As a regular part of its business, CSI requires patients to provide personal information to its healthcare customers before it provides them services. That information includes, *inter alia*, names, addresses, dates of birth, health insurance information, healthcare information, and/or Social Security numbers. CSI stores this information digitally.

31. As a HIPAA covered business entity (*see infra*), CSI is required to implement adequate safeguards to prevent unauthorized use or disclosure of Personal Information, including by implementing requirements of the HIPAA Security Rule[6] and to report any unauthorized use or disclosure of Personal Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

32. CSI's Privacy Policy states that it has "adopt[ed] appropriate data collection, storage and processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of your personal information. . . and data stored" on CSI's network.[7]

33. However, CSI did not maintain adequate security to protect its systems from infiltration by cybercriminals, and it waited nearly three months to disclose the Data Breach publicly.

34. Plaintiff and the Class Members are, or were, patients of CSI's healthcare provider customers and entrusted CSI with their Private Information on the condition that it be maintained as confidential and be used only for legitimate business uses.

B. CSI is a HIPAA Covered Business Associate

35. CSI is a HIPAA covered business associate that provides services to various health care providers (i.e., HIPAA "Covered Entities"). As a regular and necessary part of its business, CSI collects and custodies the highly sensitive PII of its clients' patients and health plan Members.

---

[6] The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. *See* 45 C.F.R. Part 160 and Part 164, Subparts A and C.

[7] *See* CSI Privacy Policy, https://www.officepracticum.com/privacy-policy (last accessed December 13, 2022).

CSI is required under federal and state law to maintain the strictest confidentiality of the patient's and plan Members' Private Information that it requires, receives, and collects, and CSI is further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

36. As a HIPAA covered business entity, CSI is required to enter into contracts with its Covered Entities to ensure that it will implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule[8] and to report to the Covered Entities any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

37. As a condition of receiving CSI's services, CSI requires that Covered Entities and their patients and plan Members, including Plaintiff and Class Members, entrust it with highly sensitive personal information. Due to the nature of CSI's business, which includes providing brand management, local marketing, marketing execution, print production and supply chain logistics, CSI would be unable to engage in its regular business activities without collecting and aggregating Private Information that it knows and understands to be sensitive and confidential.

38. CSI advertises its services to pediatrician offices as solutions for, among other issues: "increas[ing] practice revenue", "[h]elps [pediatricians] increase payment per visit", and "[m]inimizing administrative tasks and increasing patient engagement".[9]

[8] The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. *See* 45 C.F.R. Part 160 and Part 164, Subparts A and C.

[9] https://www.officepracticum.com/why-choose-op/client-results (last accessed December 13, 2022).

39. CSI's website touts security as a main feature of its software, stating that "Protecting your patient records from cyber attacks is everyone's concern" and that doing so is "paramount to a good doctor-patient relationship".[10] CSI touts that clients and patients "can place a high degree of trust behind the accuracy and integrity of the information you are storing and accessing with [CSI]. [CSI] not only meets, but exceeds best practices and industry standards for data security and preservation. [CSI's Data] is hosted in a maximum security AWS environment, that utilizes the latest and greatest hardware available."[11]

40. In the scenario of a Data Breach, CSI further touts that: "Our Cloud team is notified about any authorized or unauthorized access and changes to your systems, servers, or network appliances. Data is encrypted twice, and we run a minimum of at least two different anti-virus products to give you an added layer of security so you have peace of mind that we are looking after your most important business asset: your practice data."[12]

41. CSI's Privacy Policy on its website states that CSI uses "appropriate data collection, storage and processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of your personal information, username, password, transaction information and data stored on OP Services."[13]

42. Plaintiff and Class Members are or were patients whose medical records were maintained by, or who received health-related or other services from, CSI through its healthcare provider customers, and directly or indirectly entrusted CSI with their Private Information. Plaintiff and Class Members reasonably expected that CSI would safeguard their highly sensitive information and keep their Private Information confidential.

---

[10] https://www.officepracticum.com/why-choose-op/security (last accessed December 13, 2022).
[11] *Id.*
[12] *Id.*
[13] https://www.officepracticum.com/privacy-policy (last accessed December 13, 2022).

C. The Data Breach Compromised Plaintiffs' and Class Members' Private Information

43. On or about August 26, 2022, according to the notice CSI provided to Plaintiff and Class Members, CSI discovered "a data anomaly on [CSI's] internal network."[14] It launched an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity.

44. CSI's investigation determined, on September 13, 2022, that there was unauthorized access to certain CSI servers and that "some of that data was removed by the unauthorized party."

45. CSI did not publicly announce the Data Breach until almost three months later. On or around that time, CSI began to notify patients via letter about the data breach that CSI detected in August 2022. The press release CSI posted on its website states that the patient information compromised in the Data Breach included: (1) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth); (2) Social Security Numbers ("SSNs"), (3) health insurance information (payer name, payer contract dates, policy information including type and deductible amount and subscriber number); (4) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); and (5) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider). . . Information of a parent, guardian, or guarantor may also have been impacted by the incident."

46. CSI's notice letter also vaguely describes the measures it took following its discovery of the Data Breach, stating only that:

[14] *See* n.1, *supra.*

> As soon as we discovered the incident, we immediately took action to stop the unauthorized activity. This included a password reset of all corporate accounts and moving all patient data used for data conversion and troubleshooting into an environment with even greater security. Connexin also retained a third-party cybersecurity forensic firm to investigate the issue and is working with law enforcement to investigate the incident. In response to this incident, Connexin has enhanced its security and monitoring as well as further hardened its systems as appropriate to minimize the risk of any similar incident in the future.

47. CSI's notice omits pertinent information including how long criminals gained access to the encrypted files on its systems, what computer systems were impacted, the means and mechanisms of the cyberattack, the reason for the three month delay in notifying Plaintiff and Class Members of the Data Breach, how it determined that the Private Information had been "removed" and of particular importance to Plaintiff and Class Members, what actual steps CSI took following the Data Breach to secure its systems and prevent further cyberattacks.

48. Based on CSI's acknowledgment that personal information was "accessed by the unauthorized actor," it is evident that unauthorized criminal actors did in fact access CSI's network and exfiltrate Plaintiff's and Class Members' Private Information in an attack designed to acquire that sensitive, confidential, and valuable information.

49. The Private Information contained in the files accessed by cybercriminals appears not to have been encrypted because if properly encrypted, the attackers would have acquired unintelligible data and would not have "accessed" Plaintiff and Class Members Private Information.

50. CSI initially identified 119 healthcare insurance companies and healthcare services providers involved in the data breach, which is potentially subject to increase as new details emerge.[15] Forest Hill Pediatrics submitted a report regarding the CSI Data Breach to the Health

[15] *119 Pediatric Practices Affected by Breach at EHR Vendor – 2.2 Million Patients Affected*, HIPAA JOURNAL (Nov. 30, 2022), available: https://www.hipaajournal.com/2-2-million-patients-119-pediatric-practices-connexin-software-breach/ (last accessed December 13, 2022).

and Human Services Office for Civil Rights recently and confirmed that 4,958 of its Members were affected.[16]

51. On or about November 11, 2022, CSI reported the Data Breach to the Health and Human Services Office for Civil Rights and disclosed that 2,216,365 individuals were impacted in the Data Breach.[17]

52. As a HIPAA associated business entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk of which CSI was aware and knew it had a duty to guard against.

53. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients and/or plan Members, like Plaintiffs and Class Members.

54. Despite detecting the Data Breach on or around August 26, 2022, CSI was, of course, too late in the discovery and notification of the Data Breach.

55. Due to CSI's inadequate security measures and its delayed notice to victims, Plaintiff and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

56. CSI had obligations created by HIPAA, contract, industry standards and common law made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

57. Plaintiff and Class Members entrusted their Private Information to CSI's clients with the reasonable expectation and mutual understanding that CSI or anyone who used their Private Information in conjunction with the healthcare services they received would comply with

[16] *Id.*
[17] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed December 13, 2022).

obligations to keep such information confidential and secure from unauthorized access after it received such information.

58. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, CSI assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

59. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their personal information. Plaintiff and Class Members would not have allowed CSI or anyone in CSI's position to receive their Private Information had they known that CSI would fail to implement industry standard protections for that sensitive information.

60. As a result of CSI's negligent and wrongful conduct, Plaintiff's and Class Members' highly confidential and sensitive Private Information was left exposed to cybercriminals.

D. Defendant Was Obligated Under HIPAA to Safeguard the Private Information

71. CSI is a covered business associate under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

72. CSI is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[18] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

[18] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

73. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

74. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

75. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

76. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

77. HIPAA's Security Rule requires CSI to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

78. HIPAA also requires CSI to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, CSI is required

under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

79. HIPAA and HITECH also obligated CSI to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

80. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires CSI to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[19]

81. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

82. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

83. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed

[19] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited December 13, 2022) (emphasis added).

guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[20] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says, "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[21]

E. CSI Failed to Follow FTC Guidelines

84. CSI was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

85. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

86. According to the FTC, the need for data security should be factored into all business decision-making.

87. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

[20] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited December 13, 2022).
[21] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last visited December 13, 2022).

88. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

89. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

90. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

91. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

92. CSI failed to properly implement basic data security practices.

93. CSI's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' and plan Members Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

94. CSI was at all times fully aware of its obligation to protect the Private Information of the patients and plan Members whose Private Information it stored. CSI was also aware of the significant repercussions that would result from its failure to do so.

F. CSI Failed to Comply with Industry Standards

95. As described above, experts studying cybersecurity routinely identify healthcare providers and their business associates as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

96. Several best practices have been identified that at a minimum should be implemented by HIPAA covered business entities like CSI, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

97. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; protecting against any possible communication system; and training staff regarding critical points.

98. CSI failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

99. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and CSI failed to comply with these accepted standards, thereby opening the door to cybercriminals and causing the Data Breach.

G. CSI Owed Plaintiff and Class Members a Duty to Safeguard Their Private Information

100. In addition to its obligations under federal and state laws, CSI owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. CSI owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

101. CSI owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

102. CSI owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

103. CSI owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

104. CSI owed a duty to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

105. CSI owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

106. Had CSI remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, CSI could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

H. CSI Knew that Criminals Target Private Information

107. CSI's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the breach.

108. At all relevant times, CSI knew, or should have known, its patients', Plaintiff's, and all other Class Members' Private Information was a target for malicious actors. Despite such knowledge, CSI failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' Private Information from cyber-attacks that CSI should have anticipated and guarded against.

109. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients and/or plan Members, like Plaintiff and Class Members.

110. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[22]

[22] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last visited December 13, 2022).

111. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[23]

112. Further, a 2022 report released by IBM Security states that for 12 consecutive years the healthcare industry has had the highest average cost of a data breach and as of 2022 healthcare data breach costs have hit a new record high.[24]

113. Private Information is a valuable property right.[25] The value of Private Information as a commodity is measurable.[26] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[27] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[28] Private Information is so valuable to

---

[23] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), available: https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited December 13, 2022).
[24] *Cost of a Data Breach Report 2022*, IBM Security, available: https://www.ibm.com/downloads/cas/3R8N1DZJ (last visited December 13, 2022).
[25] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...") (last visited December 13, 2022).
[26] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192 (last visited December 14, 2022).
[27] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), Exploring the Economics of Personal Data : A Survey of Methodologies for Measuring Monetary Value | OECD Digital Economy Papers | OECD iLibrary (oecd-ilibrary.org) (last visited December 13, 2022).
[28] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last visited December 13, 2022).

identity thieves that once Private Information has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

114. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, Private Information, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

115. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[29] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[30] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[31]

116. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[32] According to a report released by the Federal Bureau of Investigation's

[29] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.") (last visited December 13, 2022).
[30] *Id.*
[31] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010, 5:00 AM), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims (last visited December 13, 2022).
[32] Adam Greenberg, *Health insurance credentials fetch high prices in the online black market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market (last visited December 13, 2022).

("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[33]

117. Criminals can use stolen Private Information to extort a financial payment by "leveraging details specific to a disease or terminal illness."[34] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion…By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[35]

118. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[36]

119. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

120. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system

---

[33] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf (last visited December 13, 2022).
[34] *See* n.26, *supra*.
[35] *Id.*
[36] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1 (last visited December 13, 2022).

is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[37]

121. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[38]

122. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[39]

123. CSI was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[40]

---

[37] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last accessed December 13, 2022).

[38] *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited December 13, 2022).

[39] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack, Security Magazine* (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited December 13, 2022).

[40] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited December 13, 2022).

124. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[41]

125. As implied by the above AMA quote, stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiffs and Class Members.

126. CSI was on notice that the federal government has been concerned about healthcare company data encryption practices. CSI knew its employees accessed and utilized protected health information in the regular course of their duties, yet it appears that information was not encrypted.

127. The OCR urges the use of encryption of data containing sensitive personal information. As far back as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, formerly OCR's deputy director of health information privacy, stated in 2014 that "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[42]

---

[41] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited December 13, 2022).

[42] "Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html (December 13, 2022).

128. As a HIPAA covered business associate, CSI should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Private Information stored in its unprotected files.

I. Theft of Private Information Has Grave and Lasting Consequences for Victims

129. Theft of Private Information is serious. The FTC warns consumers that identity thieves use Private Information to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[43]

130. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[44] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.[45]

---

[43] *See What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER ADVICE, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last visited December 13, 2022).

[44] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[45] Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last visited December 13, 2022).

131. With access to an individual's Private Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture, using the victim's name and SSN to obtain government benefits, or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[46]

132. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the Private Information stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members.

133. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on dark web, black-markets for years.

134. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.

---

[46] *See Warning Signs of Identity Theft*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited December 13, 2022).

135. The Private Information exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and substantial. As the FTC has reported, if cyber thieves get access to a person's highly sensitive information, they will use it.[47]

136. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number:** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refund, employment—even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your lift in so many ways. [48]

137. For instance, with a stolen Social Security number, which is only one subset of the Private Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[49]

138. Identity thieves can use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give

[47] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info (last visited December 13, 2022).
[48] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 15, 2017, https://www.usatoday.com/story/money/personalfinance/2017/11/15/5-ways-identity-thief-can-use-your-social-security-number/860643001/ (last visited December 13, 2022) (emphasis added).
[49] *Id.*

the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

139. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like CSI is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

140. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[50] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[51]

141. The medical information, PHI, which was exposed is also highly valuable. PHI can sell for as much as $363 according to the Infosec Institute.[52]

142. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to PII, they *will use it.*[53]

[50] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web (last visited December 13, 2022).
[51] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last visited December 13, 2022).
[52] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at:* https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited December 13, 2022).
[53] *Id.*

143. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[54] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[55][56] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[57]

144. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise in the Data Breach and has likely been made available on the dark web as it holds significant value for the threat actors. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now in the hands of identity thieves, and the rarity of the Data has been lost, thereby causing additional loss of value.

145. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[58]

146. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to

---

[54] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed December 14, 2022).
[55] https://datacoup.com/ (last accessed December 14, 2022).
[56] https://digi.me/what-is-digime/ (last accessed December 14, 2022.)
[57] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed December 14, 2022).
[58] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last visited December 13, 2022).

demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the victim has suffered the harm.

147. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[59]

148. Theft of PII is even more serious when it includes theft of PHI. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

149. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[60] "Medical

[59] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 PM), https://time.com/5643643/capital-one-equifax-data-breach-social-security/ (last visited December 13, 2022).

[60] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last visited December 13, 2022).

identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum.[61] "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[62]

150. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[63] The FTC also warns, "If the thief's health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use. It could also hurt your credit."[64]

151. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

---

[61] *Id*.
[62] *Id.*
[63] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIVACY FORUM 6 (Dec. 12, 2017), https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/ (last visited December 13, 2022).
[64] *Id.*

152. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[65]

153. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available.

154. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened. [66] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[67]

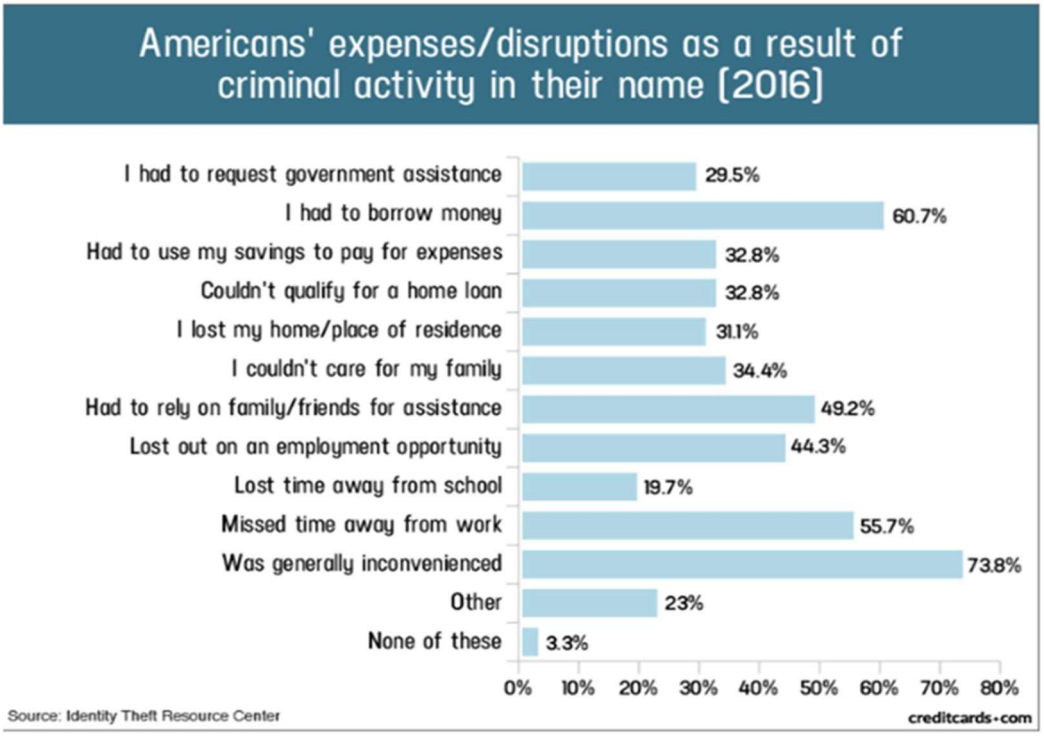
155. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[68]

156. It is within this context that Plaintiff and all other Class Members must now live with the knowledge that their Private Information is forever in cyberspace and was taken by people

[65] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), https://www.iiisci.org/Journal/PDV/sci/pdfs/IP069LL19.pdf (last visited December 13, 2022).
[66] *See* Medical ID Theft Checklist, *available at:* https://www.identityforce.com/blog/medical-id-theft-checklist-2.
[67] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages"*), *available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited December 13, 2022).
[68] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf (last visited December 13, 2022).

willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

157. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information.



158. Victims of the Data Breach, like Plaintiffs and Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[69]

159. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have had their Private Information exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and Class Members must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing

[69] *Id.*

identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

160. Plaintiff and Class Members have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;

b. Trespass, damage to, and theft of their personal property, including Private Information;

c. Improper disclosure of their Private Information;

d. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their Private Information being in the hands of criminals and having already been misused;

e. The imminent and certainly impending risk of having their confidential medical information used against them by spam callers to defraud them;

f. Damages flowing from Defendant's untimely (and in some cases, non-existent) and inadequate notification of the Data Breach;

g. Loss of privacy suffered as a result of the Data Breach;

h. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

i. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

j. The loss of use of and access to their credit, accounts, and/or funds;

k. Damage to their credit due to fraudulent use of their Private Information; and

l. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

161. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be wholly incapable of protecting Plaintiff's and Class Members' Private Information.

162. Plaintiff and Class Members also have an interest in ensuring that their personal information that was provided to CSI is removed from CSI's unencrypted files.

163. Defendant itself acknowledged the harm caused by the Data Breach because it offered Plaintiff and Class Members the inadequate 12 months of identity theft monitoring services. This limited identity theft monitoring is, however, inadequate to protect Plaintiff and Class Members from a lifetime of identity theft risk. Moreover, once the service terminates after 12 months, Plaintiff and Class Members will be forced to pay out of pocket for necessary identity theft monitoring services.

164. Defendant further acknowledged, in its notice to Plaintiff and other Class Members, that, in response to the Data Breach, CSI "hardened its systems as appropriate to minimize the risk of any similar incident in the future."[70]

165. The letter further acknowledged that the Data Breach would cause inconvenience to affected individuals by providing numerous "steps" for Class Members to take in an attempt to mitigate the harm caused by the Data Breach,[71] and that financial harm would likely occur, stating: "We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements."

166. At CSI's suggestion, Plaintiffs are trying to mitigate the damage that CSI has caused them. Given the kind of Private Information CSI made accessible to hackers, however, Plaintiffs are certain to incur additional damages. Because identity thieves have their Private Information, Plaintiffs and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[72] None of this should have happened.

167. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. For this reason, Defendant knew or should have known about these dangers and strengthened its data

[70] *See* n. 1, *supra.*
[71] *Id.*
[72] *What happens if I change my Social Security number?*, LEXINGTON LAW (Aug. 10, 202), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html (last visited December 13, 2022).

security accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

J. The Data Breach Was Foreseeable

168. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[73] Yahoo,[74] Marriott International,[75] Chipotle, Chili's, Arby's,[76] and others.[77]

169. Companies providing services to the healthcare industry, such as CSI, have been prime targets for cyberattacks. As early as August 2014, the FBI specifically warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[78] Here, as Defendant explained in the letter it sent to Plaintiffs, the data compromised in

[73] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/ (last visited December 13, 2022).
[74] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html (last visited December 13, 2022).
[75] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/ (last visited December 13, 2022).
[76] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b (last visited December 13, 2022).
[77] *See, e.g.*, Michael Hill and Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Nov. 8, 2022)), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (last visited December 13, 2022).
[78] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idINKBN0GK24U20140820 (last visited December 13, 2022).

the Breach included: "health insurance information (payer name, payer contract dates, policy information including type and deductible amount and subscriber number)"; "medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers)"; and "billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider)". Based on information obtained by Plaintiffs, CSI processes health information for major insurance companies, including We Care Pediatrics, PC and Fox Pediatrics, PLLC, among others.

170. CSI should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the Private Information that it collected and maintained.

171. Indeed, CSI's Privacy Policy states the following:

> We adopt appropriate data collection, storage and processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of your personal information, username, password, transaction information and data stored on [CSI's Servers].[79]

172. CSI's assurances of maintaining high standards of cybersecurity make it evident that CSI recognized it had a duty to use "commercially acceptable" measures to protect the Private Information that it collected and maintained. Yet, it appears that CSI did not meaningfully or comprehensively use the reasonable measures, including the "commercially acceptable" means it claims to utilize.

173. CSI was clearly aware of the risks it was taking and the harm that could result from inadequate data security.

[79] https://www.officepracticum.com/privacy-policy (last accessed Dec. 13, 2022).

K. CSI Could Have Prevented the Data Breach

174. Data disclosures and data breaches are preventable.[80] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[81] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised[.]"[82]

175. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[83]

176. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[84] The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-

---

[80] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[81] *Id.* at 17.
[82] *Id.* at 28.
[83] *Id.*
[84] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personal-information.pdf (last visited December 13, 2022).

approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

177. Upon information and belief, CSI failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, CSI also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

178. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[85]

179. To prevent and detect malware attacks, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

[85] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited December 13, 2022)

- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[86]

180. Further, to prevent and detect malware attacks, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

[86] *Id.* at 3-4.

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) ….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[87]

[87] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited December 13, 2022).

181. In addition, to prevent and detect ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials
- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise;
- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- **Build credential hygiene**
  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events
- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[88]

[88] *See* "Human-operated ransomware attacks: A preventable disaster," (Mar. 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited December 13, 2022).

182. Given that CSI was storing the Confidential Information of more than two million individuals, CSI could and should have implemented all of the above measures to prevent and detect ransomware attacks.

183. Specifically, among other failures, CSI had far too much confidential but unencrypted information held on its systems. Such Private Information should have been segregated into an encrypted system.[89] Indeed, the United States Department of Health and Human Services' Office for Civil Rights urges the use of encryption of data containing sensitive personal information, stating "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[90]

184. In sum, this Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all confidential information.

185. Plaintiff and Class Members entrusted their Private Information to CSI as a condition of receiving healthcare related services from CSI's clients. Plaintiff and Class Members understood and expected that CSI or anyone in CSI's position would safeguard their PII and PHI against cyberattacks, delete or destroy Private Information that CSI was no longer required to maintain, and timely and accurately notify them if their Private Information was compromised.

L. Plaintiffs' and Class Members Damages

186. CSI failed to inform Plaintiff and Class Members of the Data Breach in time for them to protect themselves from identity theft.

---

[89] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, Aug. 14, 2018, https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption (last visited December 13, 2022).

[90] "Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), https://www.hcinnovationgroup.com/policy-value-based-care/article/13006731/hhs-stolen-laptops-lead-to-important-hipaa-settlements (last visited December 13, 2022).

187. CSI stated that it discovered the Data Breach on August 26, 2022. And yet, CSI did not start notifying affected individuals until three months after it learned of the Data Breach. Even then, CSI failed to inform Plaintiff and Class Members exactly what information was exposed in the Data Breach, leaving Plaintiffs and Class Members unsure as to the scope of information that was compromised. In some cases, it may never contact Class Members because they had insufficient information, and instead directs them to a "substitute notice" they may never know about.

188. During these intervals, the cybercriminals were exploiting the information while CSI was secretly still investigating the Data Breach.

189. If CSI had investigated the Data Breach more diligently and reported it sooner, Plaintiff and the Class could have taken steps to protect themselves sooner and to mitigate the damages caused by the Data Breach.

190. In the Notice Letter, CSI makes an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' Private Information.

191. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

192. As a direct and proximate result of CSI's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses

such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

193. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on the acquired Private Information, as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

194. Plaintiff and Class Members have and will also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

195. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity presently and for years to come.

196. Plaintiff and Class Members suffered actual injury from having their Private Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of their Private Information, a form of property that CSI obtained from Plaintiff and Class Members; (b) violation of their privacy rights; (c) imminent and impending injury arising from the increased risk of identity theft and fraud; and (d) emotional distress.

197. Further, as a result of CSI's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy with respect to that information.

198. As a direct and proximate result of CSI's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at an increased present, continuing and imminent increased risk of future harm.

199. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of CSI, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online, is properly encrypted, and that access to such data is password protected.

200. Many failures laid the groundwork for the occurrence of the Data Breach, starting with CSI's failure to incur the costs necessary to implement adequate and reasonable cyber security

training, procedures and protocols that were necessary to protect Plaintiff's and Class Members' Private Information.

201. CSI maintained the Private Information in an objectively reckless manner, making the Private Information vulnerable to unauthorized disclosure.

202. CSI knew, or reasonably should have known, of the importance of safeguarding Private Information and of the foreseeable consequences that would result if Plaintiff's and Class Members' Private Information was stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of a breach.

203. The risk of improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to CSI, and thus CSI was on notice that failing to take necessary steps to secure Plaintiff's and Class Members' Private Information from that risk left the Private Information in a dangerous condition.

204. CSI disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that the Private Information was protected against unauthorized intrusions and properly dealing with a ransomware attack; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' Private Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

CLASS ALLEGATIONS

205. Plaintiff brings this class action on behalf of herself and A.B.T., a minor, and all Members of the following Class of similarly situated persons pursuant to Federal Rule of Civil Procedure 23. The proposed Class is defined as:

> All persons in the United States and its territories whose Private Information was compromised in the Data Breach detected by CSI on or about August 26, 2022.

206. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

207. Numerosity: The Members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable. As noted above, CSI reported that approximately 2.2 million individuals' information was exposed in the Data Breach.

208. Commonality and Predominance: Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. Such common questions of law or fact include, *inter alia*:

a. Whether CSI had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' Private Information from unauthorized access and disclosure;

b. Whether CSI's actions and its lax data security practices used to protect Plaintiff's and Class Members' PII and PHI violated the FTC Act, HIPAA, and/or other state laws and/or CSI's other duties discussed herein;

c. Whether CSI failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and Class Members;

d. Whether Plaintiff and Class Members suffered injury as a proximate result of CSI's negligent actions or failures to act;

e. Whether CSI failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' Private Information;

f. Whether an implied contract existed between Class Members and CSI providing that CSI would implement and maintain reasonable security measures to protect and secure Class Members' Private Information from unauthorized access and disclosure;

g. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and Class Members;

h. Whether CSI's actions and inactions alleged herein constitute gross negligence;

i. Whether CSI breached its duties to protect Plaintiff's and Class Members' Private Information; and

j. Whether Plaintiff and all other Members of the Class are entitled to damages and the measure of such damages and relief.

209. CSI engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of A.B.T. and all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

210. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed Members of the Class, had Private Information compromised in the Data Breach. Plaintiff and Class Members were injured by the same wrongful acts, practices, and omissions committed by CSI, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

211. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class Members. Plaintiff is an adequate representative of the Class in that neither she nor A.B.T. have interests adverse to, or in conflict with, the Class they seek to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

212. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against CSI, so it would be impracticable for Class Members to individually seek redress from CSI's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

213. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

214. CSI owed a duty to Plaintiff and all other Class Members to exercise reasonable care in safeguarding and protecting their Private Information in its possession, custody, or control.

CSI's duty arose independently from any contract to protect Plaintiff's and Class Members' Private Information.

215. CSI's duty to use reasonable care arose from several sources, including but not limited to those described below.

216. CSI had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of CSI's inadequate security measures. By receiving, maintaining, and handling Plaintiff's and Class Members' Private Information that is routinely targeted by criminals for unauthorized access, CSI was obligated to act with reasonable care to protect against these foreseeable threats.

217. CSI's duty also arose from CSI's position as a business associate. CSI holds itself out as a trusted business associate of its client-healthcare and -health insurance providers, and thereby assumed a duty to reasonably protect the Private Information it obtains from its clients. Indeed, CSI, which receives, maintains, and handles the private Information from its clients was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

218. CSI knew, or should have known, the risks of collecting and storing Plaintiff's and all other Class Members' Private Information and the importance of maintaining secure systems. CSI knew, or should have known, of the many data breaches that targeted healthcare providers in recent years.

219. Given the nature of CSI's business, the sensitivity and value of the Private Information it maintains, and the resources at its disposal, CSI should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

220. CSI breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Private Information entrusted to it—including Plaintiff's and Class Members' Private Information.

221. It was reasonably foreseeable to CSI that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, destruction and/or dissemination of Plaintiff's and Class Members' Private Information to unauthorized individuals.

222. But for CSI's negligent conduct or breach of the above-described duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

223. As a direct and proximate result of CSI's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including

the imminent and certainly impending increased risks of medical identity theft they face and will continue to face; (vii) actual or attempted fraud; (viii) continued risk of exposure to hackers and thieves of their Personal Information which remains in CSI's possession, custody, and control; and (iv) emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

224. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

225. CSI's duties arise from HIPAA, 42 U.S.C. § 1302(d), *et seq.*

226. CSI is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

227. CSI's duties further arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

228. CSI's duties also arise from Section 5 of the FTC Act, 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as CSI, of failing to employ reasonable measures to protect and secure Private Information.

229. CSI violated HIPAA Privacy and Security Rules and Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and all other Class Members' Private Information and not complying with applicable industry standards. CSI's conduct was particularly unreasonable given the nature and amount of Private Information it obtains and stores, and the foreseeable consequences of a data breach involving Private Information including, specifically, the substantial damages that would result to Plaintiff and the other Class Members.

230. CSI's violations of HIPAA Privacy and Security Rules and Section 5 of the FTC Act constitutes negligence per se.

231. Plaintiff and Class Members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTC Act, as well as state law, were intended to protect.

232. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

233. It was reasonably foreseeable to CSI that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' Private Information to unauthorized individuals.

234. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of CSI's violations of HIPAA Privacy and Security Rules and Section 5 of the FTC Act. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and

remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the certainly impending increased risk of medical identity theft they face and will continue to face; (vi) actual or attempted fraud; (viii) continued risk of exposure to hackers and thieves of their Personal Information which remains in CSI's possession, custody, and control; and (iv) emotional distress from the unauthorized disclosure of personal Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

235. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

236. Plaintiff and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by CSI and was ultimately accessed or compromised in the Data Breach.

237. Plaintiff and Class Members conferred a monetary benefit upon CSI in the form of monies paid for healthcare services or other services. CSI's business model would not exist save for the need to ensure the security of Plaintiff's and Class Members' Private Information in order to provide print, marketing execution, and supply chain management services to client-healthcare and -health insurance providers.

238. Plaintiff and Class Members further conferred a benefit on Defendant in the form of their Private Information from which Defendant derived a substantial part of its revenue. Plaintiff and Class Members allowed Defendant to maintain their Private Information on the condition that a portion of the revenue derived from the Private Information be devoted to funding adequate data security practices. Instead, Defendant diverted those funds to its own profit and did not adequately fund reasonable data security practices.

239. The relationship between CSI and Plaintiff and Class Members is not attenuated, as Plaintiff and Class Members had a reasonable expectation that the security of their Private Information would be maintained when they provided their Private Information to CSI's client-healthcare and -health insurance providers.

240. CSI accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Upon information and belief, this financial benefit was, in part, conferred, when CSI was paid by clients to use Plaintiff's Private Information to provide print, marketing execution, and supply chain management services to CSI's client-healthcare and -health insurance providers. CSI also benefitted from the receipt of Plaintiff's and Class Members' Private Information.

241. CSI also understood and appreciated that the Private Information pertaining to Plaintiff and Class Members was private and confidential and its value depended upon CSI maintaining the privacy and confidentiality of that Private Information.

242. But for CSI's willingness to commit to properly and safely collect, maintain and security Private Information, the Private Information would not have been transferred to and entrusted to CSI. Further, if CSI had disclosed that its security measures were inadequate, CSI would not have gained the trust of its client-healthcare and -health insurance providers.

243. As a result of CSI's wrongful conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

244. CSI's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the collection, maintenance, and inadequate security of Plaintiff and Class Members Private Information, while at the same time failing to securely maintain that information from unauthorized access and compromise.

245. CSI should not be permitted to retain the money belonging to Plaintiff and Class Members. It would be unjust, inequitable, and unconscionable to retain the benefits it received and is still receiving from Plaintiff and Class Members because CSI failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

246. Plaintiff and Class Members have no adequate remedy at law and the benefit conferred upon, received, and enjoyed by CSI was not conferred officiously or gratuitously, and it would be inequitable and unjust for CSI to retain the benefit.

247. CSI should be compelled to provide for the benefit of Plaintiffs and Class Members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT IV
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Class)

248. Plaintiff and the Class Members incorporate the above allegations as if fully set forth herein.

249. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

250. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' Private Information and whether CSI is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Private Information. Plaintiff alleges that CSI's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information still in CSI's possession, custody, and control will occur in the future.

251. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. A declaration that CSI owes a legal duty to secure Private Information obtained from its client health care and health insurance providers and to timely notify Plaintiffs and Class Members of such a data breach under the common law, Section 5 of the FTC Act, and HIPAA;

b. A declaration that CSI breached and continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI; and

c. A declaration that CSI's practice of using insecure, outdated, and inadequate email and computer systems and software that are easy to hack for storage and communication of PII and PHI data between CSI and third parties is unlawful.

252. This Court should also issue corresponding prospective relief requiring CSI to:

a. cease the unlawful practices described herein, and enjoining CSI from disclosing or using PII or PHI without first adequately securing or encrypting it;

b. seek, obtain, encrypt, and retain at the conclusion of this action all existing PII and PHI in their possession or the possession of third parties and provide it to Plaintiffs and the Class Members;

c. engage a third-party ombudsman as well as internal compliance personnel to monitor, conduct, test, and audit CSI's safeguards and procedures on a periodic basis;

d. audit, test, and train its internal personnel regarding any new or modified safeguards and procedures;

e. conduct regular checks and tests on its safeguards and procedures;

f. periodically conduct internal training and education to inform internal personnel how to immediately identify violations when they occur and what to do in response;

g. meaningfully educate its former and current employees about their privacy rights by, without limitation, written statements describing with reasonable specificity the precautionary steps CSI is taking to update its security technology to adequately secure and safeguard employee PII; and

h. identify to each Class Member in writing with reasonable specificity the PII and personal information of each such Class Member that was stolen in the Data Breach.

253. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at CSI. The risk of another such breach is real, immediate, and substantial. If another breach at CSI occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

254. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to CSI if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to CSI of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and CSI has a pre-existing legal obligation to employ such measures.

255. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at CSI, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and consumers whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf A.B.T. and all other Members of the Class, respectfully request that the Court enter judgment in her favor and against CSI as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of themselves and the Class, seeks appropriate injunctive relief designed to prevent CSI from experiencing another data breach by adopting and

implementing best data security practices to safeguard Private Information and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: December 14, 2022

Respectfully submitted,

By:_____
Benjamin F. Johns

SHUB LAW FIRM LLC
Jonathan Shub (PA I.D. 53965)
Benjamin F. Johns (PA I.D. 201373)
134 Kings Hwy E., 2nd Fl
Haddonfield, NJ 08033
T: (856) 772-7200
jshub@shublawyers.com
bjohns@shublawyers.com

Gary M. Klinger*
MILBERG, COLEMAN, PHILLIPS, GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878

gklinger@milberg.com

Marc Edelson (PA I.D. 51834)
EDELSON LECHTZIN LLP
411 S. State Street, Suite N-300
Newtown, PA 18940
T: (215) 867-2399
medelson@edelson-law.com

**Pro Hac Vice Forthcoming*
Counsel for Plaintiff and the Class